SECTION 2. GCCS ARCHITECTURE AND INSTALLATION PLANNING

2.1 GCCS Architecture

The primary component of the GCCS suite is the Executive Manager Server (EMS). All user profile information, application launch information, and key system information is maintained by the EM server in the */h/data/global* file system. In most cases the */h/data/global* file system is located on and shared by the EM server, although the GCCS COE Kernel does not dictate that it will be. The baseline EM server configuration, as described in Section 6 Configuring the Executive Manager Server, also has the NIS+ server and the Sybase server, key components of the current desktop environment located on the EM server. This is highly recommended but not dictated by the GCCS COE Kernel.

The account server is where the users accounts */h/users* are stored. It can be located on any platform that has adequate disk space but should never be placed on an ORACLE Database Server at a JOPES Core Database site. It also should not be place on the EM server if at all possible. Large sites should look at having a dedicated NFS server for the users accounts and other shared file systems.

The third major component in the GCCS suite is the Oracle database server. There are currently 16 JOPES core database sites (Table 2.1) where the synchronized JOPES database resides. All JOPES users connect to one or more of these sites when executing JOPES applications. In addition to these 16 sites many sites have a local Oracle database server for running site specific, service specific, or the few GCCS non-JOPES applications requiring an Oracle database.

All sites are required to use Domain Name Services (DNSs) and consequently must have one or more DNS servers configured and operational. Sites using the GCCS Automated Message Handling System (AMHS) also have a requirement for an AMHS server. Sites using Joint Deployable Intelligence Support System (JDISS) must identify which platform will be the JDISS license server.

Auditing to NFS mounted file systems is no longer recommended. Security auditing creates large amounts of data which uses a significant amount of your network capacity. NFS writes are inherently inefficient and as a consequence impact both the security auditing server and the clients. Under no circumstances should the Oracle database servers be used as auditing servers. For optimal performance, auditing should always use local file systems. The new partition maps presented in this document provides local security auditing partitions on all SUN SPARC platforms. An audit server may still be used as a central repository to which audit records are moved.

Table 2-1-1. JOPES Core Database Sites

SITE	CINC	LOCATION
ACC	ACOM	Langley AFB, VA.
ACOM	ACOM	Norfolk, VA.
AMC	TRANSCOM	Scott AFB, IL.
ARPAC	PACOM	Fort Shafter, HI.
CENTCOM	CENTCOM	MacDill AFB, FL.
EUCOM	EUCOM	Stuttgart, GE.
FORSCOM	FORSCOM	Fort McPherson, GA.
NMCC	NMCC	Pentagon, Wash. DC.
OSF	DISA	Sterling, VA.
PACAF	PACOM	Makalapa NAS, HI.
SOUTHCOM	SOUTHCOM	Fort Amador, Panama
TRANSCOM	TRANSCOM	Scott AFB, IL.
USAFE	EUCOM	Ramstein AFB, GE.
USFK	PACOM	Korea
SOCOM	SOCOM	MacDill AFB, FL.
HQDA	HQDA	Pentagon, Wash. DC.

2.2 Installation Planning

2.2.1 Key Points

a. The Solaris 2.3 operating system can be loaded on all platforms simultaneously.

b. In most cases the Executive Manager (EM) server should be built before the GCCS COE Kernel is loaded on any other platform. The only exception to this rule is when */h/data/global* is located on another platform. In this case the */h/data/global* platform should be built first and then the EM server should be built.

c. The users account server must be built second.

d. Remaining platforms can be built in any order.

e. The DNS server should be built and activated as soon as possible. It does not have to be a GCCS platform.

f. Section 7 Building the GCCS Core System, identifies the minimum requirements for all GCCS platforms.

2.2.2 Required Information

The following information must be known prior to building any GCCS system:

a. Internet Protocol (IP) address and hostname of each platform
b. Netmask being used
c. Executive Manager server IP address
d. Account server IP address
e. NIS+ Server (usually EM server)
f. Sybase server (usually EM server)
g. Mail hosts
h. Sybase **"sa"** password
I. Oracle database server (your default Oracle database server, the local server if it exists)
j. AMHS server (if applicable)
k. JDISS License Manager Server (if applicable)
l. Default router IP address
m. DNS Domain Name
n. Primary DNS Server

o. NIS+ domain name
p. IRC server
q. NEWS server
r. HTTPD server
s. Applix License Server.

2.2.3 Installation Sequence

The sequence of steps for building a GCCS system are as follows:

a. Install Solaris 2.3 operating system as instructed in Section 3.

b. Install GCCS COE Kernel as instructed in Section 4.

c. Install SUN software packages as instructed in Section 5 (if applicable).

d. Load and initialize EM server as instructed in Section 6.

e. Load required core segments and configure platform as instructed in Section 7 (except EM server).

f. Load desired applications as directed by functional users as instructed in Sections 8-16.